CORPORATE COUNSEL
An ALM Website
corpcounsel.com | October 23, 2017

What Not to Learn From Equifax: Five Big Lessons

The Equifax data breach has been unlike any other. Its victims' did not voluntarily provide their personal information to the company, nor did they have the ability to opt out.

By Craig A. Newman

The Equifax data breach has been unlike any other. Its victims did not voluntarily provide their personal information to the company, nor did they have the ability to opt out. Big banks, credit card companies and other businesses funnel stockpiles of data on consumers' financial transactions to credit reporting firms to create profiles that determine consumer creditworthiness. So, unless you don't have a credit card, cellphone or mortgage, you are almost certainly in the databases of the big three credit reporting agencies.

A logo sign outside of the headquarters of the consumer credit rating firm Equifax in Atlanta, Georgia on September 1, 2012. The company revealed a data breach that could have comprised the personal information of up to 143 million people.

Since the massive breach was disclosed last month—exposing to hackers the personal information of more than half of our country's adult population—Equifax has scrambled to cope with an unending torrent of bad news including the "retirement" of its CEO and ouster of top information security executives, dozens of lawsuits and regulatory investigations and a 30 percent hit to its stock price.

We now live in a world of predictable "stages" of data breach grief—a procession of shock, fear and ultimately, anger at companies for not being more prepared. Still, we need to learn the lessons of the Equifax hack:

- **Perceptions and Optics Matter**. Equifax has become the new poster child for a data breach gone awry. And the optics couldn't be worse. From the nearly $2 million in insider stock sales—between the time the breach was discovered but before it was publicly disclosed—to the fact that the vulnerability exploited by the hackers was a known software flaw. There were overwhelmed call centers, a dysfunctional consumer response and a lack of clear information flowing to those affected. Equifax also had registered the domain name

equifaxsecurity2017.com, the website where customers were directed to learn more about the breach, two weeks before the breach was disclosed.

- **The message matters**. Effective communication is critical, especially when confronted with a major data security incident. It's the basic blocking and tackling of crisis management. That's especially so when the breach affects tens of millions of individuals including the lawmakers, regulators and members of the press who will be asking the tough questions. In these circumstances, "no comment" or a pithy soundbite isn't an option. The message should be thoughtful, well considered, transparent and candid. It wasn't here and nothing less could have protected the brand and the company.

- **Beware of "Red Flags."** Hindsight, of course, is 20/20. But failing to spot clues or "red flags" that would have allowed the company to connect the dots and manage its risk is another issue altogether. In a damning August 2016 report, MSCI Inc.—which selects index stocks based on its analysis of a company's performance on environmental, social and governance issues—warned that Equifax "is vulnerable to data theft and security breaches." The report said, "Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems." In fact, "Equifax's data security and privacy measures have proved insufficient in mitigating data breach events," MSCI cautioned. MSCI assigned a "zero" score to Equifax's privacy and data security on a 10-point scale and downgraded the company to its lowest rating. This report begs the broader question of what—if anything— was done in response. We don't yet know the answer.

- **When to Tell**. The company has been roundly criticized for not disclosing the breach earlier. It took Equifax 40 days from discovery to public disclosure, although some reports have suggested that the hackers accessed the Equifax database earlier than the company has acknowledged. But breach disclosure isn't that simple. Companies are subject to conflicting and often irreconcilable demands. Companies have a duty to the public markets and investors to provide prompt disclosure of material risks to their business. At the same time, breach investigations take time and it's not always clear what happened and the extent of the harm for weeks, if not months. If a company makes an early disclosure that isn't accurate, it will likely be on the receiving end of a lawsuit or enforcement action for a misleading disclosure.

Then there's law enforcement. To avoid tipping off perpetrators to a continuing breach investigation, law enforcement often encourages companies to keep a breach confidential so they can catch the bad guys. This puts companies in a proverbial "Catch 22." Unfortunately, the SEC has only issued "guidance" to companies on when to disclose an incident to investors, and that is six years ago—a lifetime in the data security world. The securities laws do not define when an intrusion requires disclosure. Until the SEC brings more clarity to the breach disclosure issue, companies will need to do their best to balance these competing demands.

- **Preparation, Preparation & Preparation.** On all levels, the Equifax breach underscores the need for comprehensive preparation for a major data security incident. Preparation should include every stakeholder, department and business unit likely affected by a large-scale event: legal, human resources, internal communications, investor relation, information technology, company leadership, key outside advisers (counsel, forensics firm and crisis communications firm) and the board. And preparation should be practiced. A real data breach isn't the time to dust off an incident response plan for the first time. With data breaches, practice might not make perfect but it will certainly help manage the increasing legal, regulatory and headline risk that comes with a wide-scale incident.

These lessons are hardly new but perhaps that's the point. By any measure, the Equifax breach has been a debacle. But the good news is that it provides a teachable moment and we all need to learn from this—and soon.

Craig A. Newman *is a partner with Patterson Belknap Webb & Tyler in New York and chairs the firm's privacy and data security practice group.*